STORMSHIELD

SOLUTION BRIEF

PROTECT CRITICAL INFRASTRUCTURE

Stormshield Network Security + Airbus Cybersecurity Orion Malware

A 100% on-premise solution

Multilayer protection

Expert analysis tools

In sensitive environments, information systems cannot always be Internet-connected. And for regulatory reasons, data confidentiality doesn't allow transit through unmanaged environments. This protects them from a number of risks but rules out the benefits of cloud-hosted sandboxed environments, which offer more effective protection against complex attacks. Targeted cyberattacks targeting sensitive environments are designed to bypass conventional antivirus solutions by combining several attack vectors, including offline.

A 100% on-premise solution against complex cyberattacks

OPTIMAL PROTECTION AGAINST THREATS

Preventing, blocking and defending against multi-vector attacks requires solutions that combine multiple technologies and techniques. That is why Stormshield extended Stormshield Network Security capabilities with Breach Fighter, a sandboxing technology hosted in the cloud dedicated to small and medium businesses. The comprehensive Stormshield Network Security and Orion Malware solution was designed to respond to environment unconnected to Internet, sensitives data context or needs for flexibility and advanced analysis tools.

Boasting malicious code and unknown threats detection capabilities, Orion Malware analyses suspect files submitted by Stormshield Network Security, which also performs the network blocking function.

The information extracted from files during analysis by Orion Malware can then be used to track malware proactively. Network filtering rules can be modified based on this analysis.

Key features of Stormshield Network Security

- VPN-compatible
- Protocol-based IPS with deep application inspection
- High Availability
- Hardened form factor availability with bypass connection.
- EU restricted, NATO restricted, EAL4+ certified and ANSSI (National Cybersecurity Agency of France) qualified

Key features of Airbus Orion Malware

- Combination of multiple analysis techniques (signatures, heuristics, machine learning, sandboxing)
- Modularity: addition of new static analysis components, choice of sandboxed OS (Windows XP, 7 & 10, Linux, Android)
- Simple system integration (RESTful API, ICAP, SIEM)
- Extraction of IOCs to generate detection rules or analysis
- Made in France

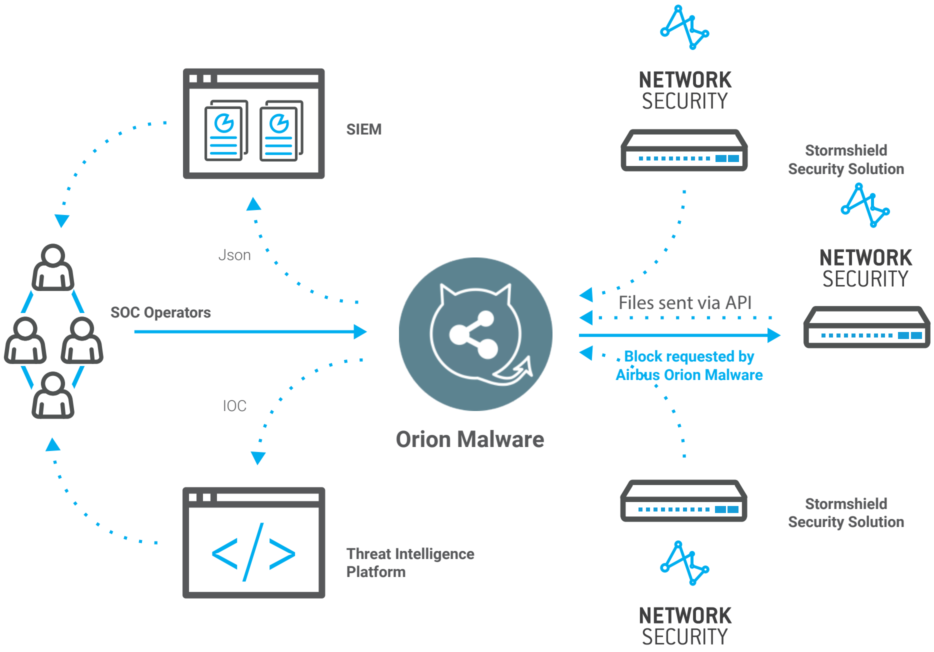
MULTILAYER PROTECTION

The Stormshield Network Security/Orion Malware solution comprises network devices capable of extracting and analysing thousands of files in a private network. Detection is underpinned by a combination of protocol-based analysis, triage by opportunistic signatures and APTs, static analysis, machine learning and dynamic analysis (sandboxing).

After each file analysis by Orion Malware, a risk assessment is conducted and the result is sent to the Stormshield Network Security appliance that submitted the file in order to block the network if necessary. A summary of the file analysis and a report is available to the user for improving his knowledge of the threat. All IOCs extracted can be exported automatically to a SIEM (syslog, JSON, API) to consolidate the knowledge of the security.

AN ON-PREMISE SOLUTION FOR SENSITIVE ENVIRONMENTS

The Stormshield Network Security/Orion Malware solution is packaged as an appliance. It can be deployed easily in sensitive environments without the need for exchanges with the cloud.


NETWORK SECURITY
SIEM
Stormshield Security Solution
NETWORK SECURITY
Json
SOC Operators
Files sent via API
Block requested by Airbus Orion Malware
IOC
Orion Malware
Stormshield Security Solution
Threat Intelligence Platform
NETWORK SECURITY

Stormshield, a wholly-owned subsidiary of Airbus CyberSecurity, offers innovative, end-to-end security solutions for the protection of IT networks (Stormshield Network Security), workstations (Stormshield Endpoint Security) and data (Stormshield Data Security).

www.stormshield.com

Version 1.0 - Copyright Stormshield 2018